Title (en)

SECURE EXPONENTIAL FUNCTION COMPUTATION SYSTEM, SECURE EXPONENTIAL FUNCTION COMPUTATION METHOD, SECURE COMPUTATION DEVICE, AND PROGRAM

Title (de)

SICHERES EXPONENTIELLES FUNKTIONSBERECHNUNGSSYSTEM, SICHERES EXPONENTIELLES FUNKTIONSBERECHNUNGSVERFAHREN, SICHERE BERECHNUNGSVORRICHTUNG UND PROGRAMM

Title (fr)

SYSTÈME DE CALCUL DE FONCTION EXPONENTIELLE SÉCURISÉE, PROCÉDÉ DE CALCUL DE FONCTION EXPONENTIELLE SÉCURISÉE, DISPOSITIF DE CALCUL SÉCURISÉ ET PROGRAMME

Publication

EP 4095828 A1 20221130 (EN)

Application

EP 20915352 A 20200120

Priority

JP 2020001676 W 20200120

Abstract (en)

In secure computation, an exponential function is calculated at high speed. A secure exponential function computation system (100) receives [a] as an input and calculates [exp (a)]. The minimum value subtraction unit (11) calculates [a']: = [a] - μ. A bit decomposition unit (12) generates a bit representation [a'₀], ..., [a'_{u - 1}] of u upper bits of a' from [a']. A selective product unit (13) calculates a total product [f'] of values that are [a'_i?f_i:1]. An upper bit calculation unit (14) calculates a total product [ε'] of [a'_i?2^{ε_i}:1] for 0 ≤ i < u. A lower bit calculation unit (15) calculates [a'_ρ]: = [a'] - ∑2^{i - t}[a'_i]. An exponential function calculation unit (16) calculates [w]: = [exp (a'_ρ)]. A result calculation unit (17) calculates [w][f'][ε']exp (μ).

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/10** (2006.01)

CPC (source: EP US)

G06F 21/6218 (2013.01 - US); **H04L 9/085** (2013.01 - EP); **H04L 9/16** (2013.01 - EP)

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

Designated validation state (EPC)

KH MA MD TN

DOCDB simple family (publication)

EP 4095828 A1 20221130; **EP 4095828 A4 20231018**; AU 2020424992 A1 20220714; AU 2020424992 B2 20230406; CN 114981862 A 20220830; JP 7351353 B2 20230927; JP WO2021149100 A1 20210729; US 2023069892 A1 20230309; WO 2021149100 A1 20210729

DOCDB simple family (application)

EP 20915352 A 20200120; AU 2020424992 A 20200120; CN 202080093539 A 20200120; JP 2020001676 W 20200120; JP 2021572122 A 20200120; US 202017790534 A 20200120